

FIRST DRAFTS LEITFADEN ZUM THEMA

Verifizierung von Online- Informationen

Januar 2020

FIRSTDRAFT

INHALTSVERZEICHNIS

	Einführung	7
KAPITEL 1	Wichtige Grundlagen	11
KAPITEL 2	Herkunft	27
KAPITEL 3	Quelle	35
KAPITEL 4	Datum	41
KAPITEL 5	Ort	45
KAPITEL 6	Motivation	51

ÜBER DIE AUTORIN

Shaydanay Urbani ist Autorin und wissenschaftliche Mitarbeiterin bei First Draft, wo sie sich mit Desinformationen beschäftigt und weltweit Schulungen für Journalisten durchführt, die sich mit Verifizierung und verantwortungsvoller Berichterstattung befassen. Ihre Erfahrungen und Kenntnisse umfassen Gerichtsreportage, Nahostsprachen und Politik sowie Lebensmittelgesetze. Sie hat einen Master in Journalismus von The City University of New York.

In ihrer Freizeit tanzt sie in einem professionellen Salsa-Team in New York City.

2. Ausgabe, Erstveröffentlichung Oktober 2019
Herausgegeben von Alastair Reid und Victoria Kwan
Produziert von Tommy Shane
Design: Imagist

Dieses Werk ist unter der Creative Commons Attribution-Non-Commercial-NoDerivatives 4.0 International License lizenziert. Eine Kopie dieser Lizenz finden Sie unter: <http://creativecommons.org/licenses/by-nc-nd/4.0/>

Danksagungen

Vielen Dank an unser Team mehrsprachiger Journalisten, die bei der Überprüfung der Übersetzungen in mehrere Sprachen unter der Leitung von First Drafts Emma Dobinson mitgewirkt haben: Pedro Noel (Brazillianisch), Carlotta Dotto (Italienisch), Marie Bohner (Französisch), Laura Garcia (Spanisch), Nadin Rabaa von GNL Berlin (Deutsch) und Professor Umesh Arya von DataLEADS (Hindi).

Die Originalversion für diesen Kurs wurde auf Englisch im Oktober 2019 veröffentlicht.

Diese DEUTSCHE Version wurde von Global Lingo übersetzt und von Mitgliedern des First Draft-Teams überprüft. Diese übersetzte Version wurde im Juni 2020 veröffentlicht.

Alle Leitfäden in deutscher Sprache

Einleitung

Die Verifizierung von Online-Inhalten kann einschüchtern, aber sie durchzuführen, ist nicht schwierig. Gute Verifizierung braucht vor allem Wiederholung, Ausdauer und digitale Tools gepaart mit etwas Kreativität. Mittlerweile gibt es sehr viele Tricks und Tools für die Verifizierung. Deswegen besteht die schwierigste Herausforderung darin, sich an alle verfügbaren Ressourcen zu erinnern.

Hierbei soll dieser Leitfaden helfen. Dieses kleine komprimierte Handbuch soll Sie bei dem Verifizierungsprozess unterstützen und enthält wichtige Konzepte, Checklisten und persönliche Tipps und Methoden. Vor allem aber soll es Sie mit den fünf Säulen der Verifizierung vertraut machen und dient Ihnen hoffentlich als schnelle Referenz, wie Sie jede Säule umsetzen.

Informationen verbreiten sich schnell, und Fehlinformationen lassen sich so leicht erzeugen und verbreiten, dass jeder Journalist – nicht nur die Tech-Reporter und Social-Media-Redakteure – über grundlegende Verifizierungskennnisse verfügen sollte.

Insbesondere in einer von aktuellen Nachrichten geprägten Umgebung, in der der Druck hoch ist, schnell zu berichten und die richtigen Fakten zu präsentieren. Außerdem müssen sich Newsrooms davor schützen, an der Nase herumgeführt zu werden und Unwahrheiten versehentlich an ein breites Publikum weiterzugeben. Für diejenigen, die Desinformationen verbreiten, ist die Berichterstattung durch etablierte Nachrichtenmedien das angestrebte Ziel. Sie nutzen deshalb das Netz, um Gerüchte und manipulierte Inhalte zu starten in der Hoffnung, ein breiteres Publikum zu erreichen. Weitere Informationen hierzu finden Sie in [First Drafts Leitfaden zum Thema Verantwortungsvolle Berichterstattung in Zeiten des Informationschaos¹](#).

Lassen Sie sich nicht täuschen. Lernen Sie zu verifizieren.

ZU DIESEM BUCH

Bevor Sie sich in ein Verifizierungsabenteuer stürzen, sollten Sie das erste Kapitel lesen: „Wichtige Grundlagen“. Hier sind die Konzepte aufgeführt, die Sie kennen müssen und die Ihnen Zeit und mögliche Blamagen ersparen.

Der Rest des Buches ist in fünf grundlegende Überprüfungen eingeteilt, die Sie für jeden Inhalt durchführen sollten, den Sie verifizieren möchten, egal ob es sich um einen Augenzeugenbericht, ein manipuliertes Video oder ein Meme handelt.

Von diesen Kapiteln ist „Herkunft“ das wichtigste, lesen Sie es also besonders sorgfältig. Ansonsten können Sie nach Belieben blättern oder direkt die Listen mit Tipps lesen, die für Sie relevant sind.

Verifizierung ist ein fließender Prozess, während dessen Sie immer wieder neue Hinweise und Beweisstücke finden. Fortschritte, die Sie bei einer Überprüfung erzielen, können Ihnen bei einer anderen weiterhelfen.

KAPITEL 1

Wichtige Grundlagen

Bevor Sie Online-Inhalte verifizieren, sollten Sie sich diese erste grundsätzliche Frage stellen: Ist der Inhalt, den ich betrachte, mit einem Ereignis verbunden, das tatsächlich stattgefunden hat?

In bestimmten Fällen, beispielsweise bei aktuellen Nachrichten, wollen Sie vielleicht genau das mit Ihrer Verifizierung herausfinden. Aber in anderen Fällen geht es nicht darum.

Mal angenommen, Sie fänden ein Video, von dem behauptet wird, dass es lange Warteschlangen und verärgerte Passagiere im Chicago O'Hare International Airport zeigt. Bevor Sie sich daran machen, die Person, die das Video aufgenommen hat, Datum und Uhrzeit oder Ort zu verifizieren, sollten Sie zuerst die folgende Frage stellen: Gibt es tatsächlich Berichte über Probleme am Flughafen?

Ein anderes Beispiel ist die berühmte Schlagzeile, die vor den US-Wahlen 2016 auftauchte: Papst unterstützt Donald Trump. Sie können beliebig viele Verifizierungen für die Website durchführen: Wer sie geschrieben hat, wann der Artikel veröffentlicht wurde, wie weit er sich verbreitete usw. Zuerst sollten Sie jedoch die zentrale Behauptung des Artikels prüfen.

DIE FÜNF SÄULEN DER VERIFIZIERUNG

Das Gute an Kursen zum Thema Verifizierung ist, dass sie sich einfach gliedern lassen. Denn die grundlegenden Überprüfungen, die Sie durchführen müssen, sind immer gleich, ganz egal, ob es sich um ein Augenzeugenvideo, ein manipuliertes Foto, einen Sockenpuppen-Account oder ein Meme handelt.

1. HERKUNFT

Sehen Sie den originalen Bericht, Artikel oder Inhalt?

2. QUELLE

Wer hat den Bericht bzw. Artikel erstellt oder den Originalinhalt aufgenommen?

3. DATUM

Wann wurde er erstellt?

4. ORT

Wo wurde der Account eingerichtet, die Website erstellt oder der Inhalt aufgenommen?

5. MOTIVATION

Warum wurde der Account eingerichtet, die Website erstellt oder der Inhalt aufgenommen?

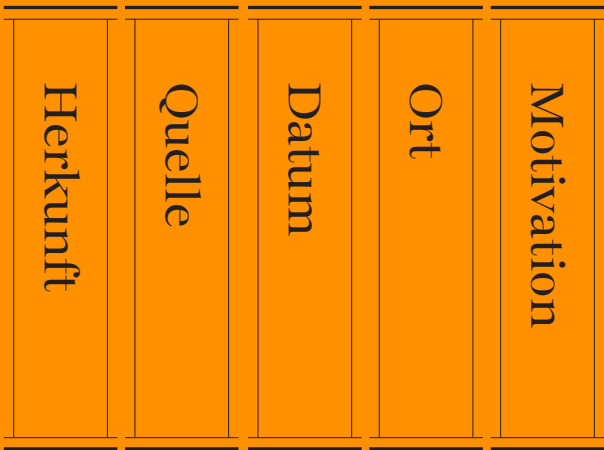
Je mehr Sie über jede Säule wissen, desto besser wird Ihre Verifizierung sein.

GEWISSEHEIT IST UNMÖGLICH

Absolute Sicherheit bei der Verifizierung ist selten. Stattdessen sucht man nach Hinweisen und sammelt Beweismaterial. Stellen Sie sich das Untersuchungsbrett eines Detektivs vor. Bruchstücke von Information werden an die Tafel geheftet: ein Ort, ein Name, eine aufschlussreiche Aussage. Linien zwischen den Hinweisen stellen ein Netz von Verbindungen dar. Genau das ist digitale Verifizierung: Dieselben alten Methoden, die Reporter und Ermittler schon immer verwendet haben, um zur Wahrheit vorzudringen, aber auf das Internet angewendet.

Finden Sie also Ihren inneren Sherlock Holmes, sammeln Sie möglichst viele Beweise, aber seien Sie sich auch bewusst, dass Sie nicht immer eine definitive Antwort erhalten. Weil uns die Gewissheit versagt bleibt, ist es umso wichtiger, dass wir offen zugeben, was wir wissen und was wir nicht wissen – insbesondere dann, wenn diese Informationen unsere Berichterstattung beeinflussen.

Die folgenden Seiten enthalten zwei Rubriken, die wir für die Verifizierung visueller Medien zusammengestellt haben – eine für Fotos und eine für Videos. Sie helfen Ihnen zu beurteilen, wie hieb- und stichfest Ihre Verifizierung ist und wo es noch Lücken gibt.



Die 5 Säulen der visuellen
Verifizierung.
Quelle: First Draft.

LEITFADEN FÜR DIE VISUELLE VERIFIZIERUNG: FOTOS

NEIN		
1. SEHEN SIE DIE ORIGINALVERSION?	Mithilfe der umgekehrten Bildersuche erhalten Sie identische Fotos, die im Netz indexiert wurden, bevor das fragliche Ereignis stattfand.	Eine umgekehrte Bildersuche führt zu ähnlichen Ergebnissen mit einigen identischen Merkmalen, was darauf hindeutet, dass es sich um eine Collage handeln könnte
2. WISSEN SIE, WER DAS FOTO AUFGENOMMEN HAT?	Es kam über eine anonyme E-Mail oder Chat-App-Nummer	Es wurde auf einem sozialen Netzwerk hochgeladen, aber der Benutzername erscheint nirgendwo sonst online. Der Hochladende möchte anonym bleiben
3. WISSEN SIE, WO DAS FOTO AUFGENOMMEN WURDE?	Ortsdaten waren nicht verfügbar und das Foto enthält keine visuellen Hinweise, um dem weiter nachzugehen	Wir haben es mit anderen Fotos verglichen, die es von der Szene gibt, aber es gibt keine Satelliten- oder Straßenansichten, um den Ort zu bestätigen
4. WISSEN SIE, WANN DAS FOTO AUFGENOMMEN WURDE?	Es wurde uns anonym zugesendet und es sind keine EXIF-Daten verfügbar	Wir haben den Zeitstempel auf dem sozialen Netzwerk überprüft, um festzustellen, wann es das erste Mal online geteilt wurde, aber wir haben keine EXIF-Daten, die bestätigen, wann es aufgenommen wurde
5. WISSEN SIE, WARUM DAS FOTO AUFGENOMMEN WURDE?	Wir wissen nicht, wer das Foto gemacht hat. Wir können also nicht einschätzen, was die Beweggründe gewesen sein könnten	Das Social-Media-Konto wurde erst vor Kurzem erstellt und/oder Suchen in den sozialen Medien ergeben, dass der Hochladende selten online postet, es gibt also wenig Beweise, die seine Bewegungen oder Beweggründe bestätigen

<p>Eine Datumssuche auf verschiedenen sozialen Netzwerken zeigt, dass es sich um die erste von vielen Versionen handelt, die online geteilt wurden, aber wir haben noch keine Bestätigung des Hochladenden erhalten</p>	<p>Wir können keine anderen Versionen im Netz finden und die allgemeine Überprüfung der Schatten und Spiegelungen deutet darauf hin, dass es nicht manipuliert wurde</p>	<p>Es wurde uns direkt zugeschickt und wir haben mit der Quelle gesprochen</p>
<p>Durch Suchen nach dem vollständigen Namen, umgekehrte Bildersuche des Profilfotos des Benutzers und/oder Untersuchung der Domain-Inhaberschaft des Blogs oder der Website konnten wir den Hochladenden identifizieren</p>	<p>Wir haben mit dem Uploader über soziale Medien kommuniziert, um zu bestätigen, dass er das Foto gemacht hat</p>	<p>Wir haben die Quelle befragt und ihre Antworten stimmten mit EXIF-Daten, Wetterberichten und ihrem eigenen digitalen Fußabdruck überein</p>
<p>Wir haben visuelle Hinweise wie zum Beispiel Schilder, Architektur und Kleidung verwendet, um die geografische Region grob zu bestimmen</p>	<p>Wir haben Landschaft und Wahrzeichen mithilfe von Karten-Tools verglichen und die Längen-/Breitenkoordinaten bestätigt</p>	<p>Die Quelle konnte andere Wahrzeichen in ihrem Blickfeld bestätigen, die mit den auf Online-Karten gezeigten übereinstimmten</p>
<p>Der Zeitstempel zeigt, dass es kurz nach dem Ereignis hochgeladen wurde, und es enthält visuelle Hinweise, die sich mit anderen Augenzeugenberichten decken</p>	<p>Wir konnten bestätigen, dass die Wetterbedingungen und alle im Bild sichtbaren Schatten mit dem von der Quelle angegebenen Zeitpunkt, Datum und Ort übereinstimmen</p>	<p>Es enthält EXIF-Daten, die zusammen mit anderen Überprüfungen bestätigen, wann es aufgenommen wurde</p>
<p>Erweiterte Suchen nach dem richtigen Namen des Hochladenden enthüllen, dass er mit einer Aktivisten- oder Interessenorganisation verbunden ist, es gibt aber keine zusätzlichen Informationen, um die Beweggründe in diesem Fall zu kennen</p>	<p>Suchen nach den Aktivitäten des Uploaders in sozialen Medien vor dem Ereignis bestätigen die Gründe für die Aufnahme des Fotos, d. h. Urlauber, Journalist, arbeitet vor Ort</p>	<p>Der Fotograf bestätigte die genauen Umstände des Fotos</p>

LEITFADEN FÜR DIE VISUELLE VERIFIZIERUNG: VIDEOS

NEIN

1. SEHEN SIE DIE ORIGINALVERSION?	Nachdem wir auf allen sozialen Netzwerken nach Schlüsselbegriffen gesucht haben, konnten wir frühere Versionen des Videos finden	Eine umgekehrte Bildersuche des Video-Thumbnail zeigt uns andere Online-Versionen, aber wir können nicht bestätigen, welche das Original ist
2. WISSEN SIE, WER DAS VIDEO AUFGENOMMEN HAT?	Es kam über eine anonyme E-Mail oder Chat-App-Nummer	Es wurde auf ein soziales Netzwerk hochgeladen, aber der Benutzername erscheint nirgendwo sonst online. Der Hochladende möchte anonym bleiben
3. WISSEN SIE, WO DAS VIDEO AUFGENOMMEN WURDE?	Es gibt nicht genügend visuelle Hinweise im Video, um zu bestätigen, wo es aufgenommen wurde	Eine Übersetzung des Begleittexts liefert Hinweise dazu, wo es gedreht wurde, aber wir konnten den Ort nicht identifizieren
4. WISSEN SIE, WANN DAS VIDEO AUFGENOMMEN WURDE?	Das Video wurde uns anonym zugesendet und es sind keine Metadaten verfügbar	Wir haben den Zeitstempel auf der ältesten Version, die auf ein soziales Netzwerk hochgeladen wurde, geprüft. Wir haben aber keine Daten, die bestätigen, wann es aufgenommen wurde
5. WISSEN SIE, WARUM DAS VIDEO AUFGENOMMEN WURDE?	Wir wissen nicht, wer das Video gedreht hat. Wir können also nicht einschätzen, was die Beweggründe gewesen sein könnten	Das Social-Media-Konto wurde erst vor Kurzem erstellt und/oder Suchen in den sozialen Medien ergeben, dass der Hochladende selten online postet, es gibt also wenig Beweise, die seine Bewegungen oder Beweggründe bestätigen

<p>Eine Suche nach dem URL-Shortcode legt nahe, dass es sich um die erste, im Netz geteilte Version handelt, aber wir konnten nicht mit dem Hochladenden sprechen</p>	<p>Wir finden keine anderen Versionen des Videos im Netz</p>	<p>Es wurde uns direkt zugeschickt und wir haben mit der Quelle gesprochen</p>
<p>Durch Suchen nach dem vollständigen Namen, umgekehrte Bildersuche des Profilfotos des Benutzers und/oder Untersuchung des Domain-Besitzers des Blogs oder der Website konnten wir den Uploader identifizieren</p>	<p>Wir haben mit dem Uploader über soziale Medien kommuniziert, um zu bestätigen, dass er das Video aufgenommen hat</p>	<p>Wir haben die Quelle befragt und ihre Antworten stimmten mit Wetterberichten, dem verwendeten Gerät und ihrem eigenen digitalen Fußabdruck überein</p>
<p>Wir haben visuelle Hinweise wie zum Beispiel Schilder, Architektur und Kleidung verwendet, um die geografische Region grob zu bestimmen</p>	<p>Wir haben Landschaft und Wahrzeichen mithilfe von Karten-Tools verglichen und die Längen-/Breitenkoordinaten bestätigt</p>	<p>Wir haben die Quelle befragt und ihre Antworten dazu, wo das Video aufgenommen wurde, stimmten mit anderen visuellen Erkennungsmerkmalen der Gebiete überein</p>
<p>Der Zeitstempel zeigt, dass es kurz nach dem Ereignis hochgeladen wurde, und es enthält visuelle Hinweise, die sich mit anderen Augenzeugenberichten decken</p>	<p>Wir haben die Quelle befragt und konnten bestätigen, dass sie zum Zeitpunkt der Videoaufnahme an diesem Ort war</p>	<p>Wir konnten bestätigen, dass die Wetterbedingungen und alle im Bild sichtbaren Schatten mit dem von der Quelle angegebenen Zeitpunkt, Datum und Ort übereinstimmen</p>
<p>Erweiterte Suchen nach dem richtigen Namen des Hochladenden enthüllen, dass er mit einer Aktivisten- oder Interessenorganisation verbunden ist, es gibt aber keine zusätzlichen Informationen, um die Beweggründe in diesem Fall zu kennen</p>	<p>Aktivitäten vor dem Ereignis bestätigen die Gründe für die Aufnahme des Videos, d. h. Urlauber, Journalist, arbeitet vor Ort</p>	<p>Wir haben mit der Quelle gesprochen, die die genauen Umstände des Videos bestätigte</p>

LOHNT SICH EINE VERIFIZIERUNG?

VERZETTELN SIE SICH NICHT

Oftmals dauert eine Verifizierung nur Minuten. In anderen Fällen kann sie zur besessenen Suche führen, die trotzdem erfolglos bleibt. Erfahren Sie, wann es Sinn macht, aufzugeben. Beachten Sie auch, dass ein zu starkes Festhalten an einer Hypothese, woher ein Inhalt stammt oder ob er wahr ist, nicht nur die Integrität Ihrer Verifizierung gefährden kann, sondern auch unheimlich zeitraubend ist.

„Wir sind alle nur Menschen und reagieren instinktiv darauf, ob ein Inhalt wahr oder falsch ist. Aber wir müssen immer skeptisch bleiben.“

Denken Sie an die alte Redakteurs-Weisheit: Selbst wenn deine Mutter sagt, sie liebt dich, überprüfe die Wahrheit der Aussage.

Das Internet ist ein weitläufiger Ort mit vielen verborgenen Winkeln. Wenn Sie zu angestrengt nach einem bestimmten Beweisstück suchen, übersehen Sie dabei vielleicht gegenteilige Beweise.

AUSBREITUNG VERSTEHEN

Berichte über Fehlinformationen sind eine schwierige Aufgabe. Studien belegen, dass sich falsche Gerüchte in manchen Fällen sogar durch schriftliche „Widerlegungen“ einprägen. Das bedeutet, dass selbst wohlgemeinte Berichte über Fehlinformationen dem Inhalt, der ansonsten

vielleicht wieder verschwunden wäre, zu einem höheren Bekanntheitsgrad verhelfen.

Wenn Sie irreführenden Inhalt verifizieren, weil Sie darüber berichten oder ihn widerlegen wollen, überlegen Sie zuerst, welche Reichweite dieser Inhalt online hat.

Wie viele Personen haben eine falsche Behauptung bereits gesehen? Mit den zur Verfügung stehenden Daten ist die Quantifizierung häufig schwierig, denn normalerweise sind das nur Angaben, wie oft geteilt, geliked, retweetet wurde, Ansichten oder Kommentare. Aber man sollte es versuchen. Selbst kleine oder Nischen-Communities können online wichtiger erscheinen.

Wenn es um einen Inhalt geht, der sehr wenig Interaktion erzeugt hat, lohnt es sich vielleicht nicht, ihn zu verifizieren oder darüber zu schreiben.

Weitere Informationen hierzu finden Sie in [First Drafts Leitfaden zum Thema Verantwortungsvolle Berichterstattung in Zeiten des Informationschaos¹](#).

TIPPS, UM ZEIT UND FRUST ZU SPAREN

DOKUMENTIEREN SIE ALLES.

Machen Sie von allem Screenshots! Inhalte können von der Host-Plattform schnell gelöscht oder entfernt werden. Es wird Sie vielleicht überraschen, wie schnell Sie wichtige Informationen verlieren können. Dokumentation ist auch deshalb wichtig, damit die Verifizierung transparent ist.

- Auf Mac OS können Sie einen Screenshot erstellen, indem Sie Command+Shift+5 drücken und dann den Cursor über den Bereich ziehen, den Sie festhalten wollen, oder indem Sie das Snipping Tool auf Windows verwenden.

- Die Verwendung eines Screenshot-Tools wie Evernote, mit dem Sie schnell Beweise sammeln können, ist manchmal hilfreich.
- Wayback Machine² ist eine Browser Extension, mit der Sie archivierte Versionen von Webseiten speichern können.
- Hunch.ly³ ist ein leistungsstarkes Tool, mit dem Sie die gesamte Untersuchung dokumentieren können, indem Sie Screenshots Ihres Browsers automatisch hineinziehen und katalogisieren. Es ist ein kostenpflichtiges Tool und deshalb nicht für jedermann geeignet, aber wenn Sie ein zuverlässiges System zur Dokumentation von Untersuchungen benötigen, dann lohnt sich die Anschaffung vielleicht.

SUCHE NICHT VERGESSEN

Es gibt viele beeindruckende Tools für die Verifizierung und über viele sprechen wir in diesem Handbuch. Manchmal genügt allerdings bereits eine einfache Google-Suche.

TELEFONIEREN NICHT VERGESSEN

In vielen Situationen gibt es ein Best Case Szenario: Sie finden eine Telefonnummer oder E-Mail-Adresse einer Quelle, so dass Sie direkt mit ihr Kontakt aufnehmen und sie über den geteilten Inhalt fragen können. Selbst eine einfache SMS kann ein Privatgespräch starten, in dem Sie viel mehr herausfinden, als es sonst der Fall wäre.

EINE TOOLBOX EINRICHTEN

Wenn Sie viele Verifizierungen oder andere digitale Recherchen durchführen, lohnt sich die Einrichtung eines Lesezeichensystems, das Ihre bevorzugten Websites beinhaltet. Wie bereits erwähnt, besteht eine der größten Herausforderungen darin, sich an die Tools zu erinnern, die zur Verfügung stehen.

Es ist gut, Lesezeichen für Ordner in einem Browser zu setzen, aber wir speichern Verifizierungstools am liebsten mit einer [Start.me](#)⁴ Seite. Die Seite zeigt alle Ihre Lesezeichen übersichtlich an und ermöglicht Ihnen, schnell neue Ressourcen einzurichten und ständig neue hinzuzufügen. Sie können sie als Ihre Startpage verwenden oder an anderer Stelle mit einem Lesezeichen markieren.

GLEICHZEITIG ÄHNLICHE INHALTE IM BLICK BEHALTEN

Bei der Verifizierung eines Inhalts kann es nützlich sein, ein Monitoring-Dashboard und ein Benachrichtigungssystem einzurichten, damit Sie sehen können, wenn ähnliche Inhalte auftauchen. Sie können Schlüsselbegriffe und Formulierungen aus dem untersuchten Inhalt verwenden, um zum Beispiel eine Suchspalte in Tweetdeck oder eine Liste von Accounts, die häufig mit Ihrer Quelle interagieren, einzurichten. Weitere Informationen, wie Sie soziale Medien effektiv beobachten, finden Sie in [First Drafts Leitfaden zum Thema Nachrichtenbeschaffung und Monitoring sozialer Netzwerke](#)⁴.

AUF DEM NEUESTEN STAND SEIN

Verifizierungsmethoden verändern sich ständig. Tech-Plattformen modifizieren ihre Datenschutzeinstellungen, Recherche-Tools werden entfernt und neue entwickelt. Wenn Sie Schritt halten möchten, sollten Sie Ihre Toolbox regelmäßig aktualisieren oder sich die neusten Methoden der Verifizierungs- und Open Source Intelligence (OSINT) Community durchlesen. Es gibt viele öffentliche OSINT-/Verifizierungslisten auf Twitter, denen Sie folgen können, um dies zu tun. Siehe [First Drafts Leitfaden zum Thema Nachrichtenbeschaffung und Monitoring](#) für weitere Informationen, wie Sie Listen finden und anlegen.

SICHERHEIT

Es gibt viele Sicherheitsmaßnahmen, die Sie bei der Durchführung von digitalen Untersuchungen ergreifen sollten, insbesondere dann, wenn Sie sich auf geschlossenen und anonymen Plattformen wie Discord aufhalten. Hier sind einige Tipps, die Sie beachten sollten:

- Stellen Sie sicher, dass Ihre persönliche digitale Sicherheit gewährleistet ist. Verwenden Sie möglichst einen Passwort-Manager.
- Überprüfen Sie Ihren eigenen digitalen Fußabdruck und die Datenschutzeinstellungen aller ihrer Social-Media-Konten. Wie viel könnte jemand über Sie, Ihre Familie und Ihre Freunde über Ihre Konten herausfinden?
- Ziehen Sie ein VPN und einen anonymen Webbrowser wie Tor in Betracht.
- Wenn Sie auf geschlossenen und anonymen Plattformen aktiv sind oder dort mit anderen interagieren, seien Sie vorsichtig, wie viele personenbezogene Informationen Sie offenlegen.

ETHISCHE GRUNDSÄTZE UND STANDARDS GELTEN WEITER

Digitale Berichterstattung bedeutet nicht, dass allgemeine ethische Grundsätze und Standards des Journalismus nicht länger gelten. Stattdessen könnte es sogar neue ethische Überlegungen geben, an die Sie noch gar nicht gedacht haben. Hier einige Punkte und Fragen zum Thema:

- Eine E-Mail ist nicht so gut wie ein Interview, das Sie persönlich durchgeführt haben, und dasselbe gilt für ein Zitat aus einem Post im Internet. Sprechen Sie mit den Personen direkt, wenn das möglich ist.

- Manche Verifizierungstools machen sich die Art und Weise zunutze, wie Social-Media-Plattformen Datenschutzeinstellungen verschleiern, was dazu führt, dass Personen Dinge teilen, von denen sie nicht wussten, dass sie öffentlich sind. Vermeiden Sie es, unnötig in das Privatleben anderer einzudringen.
- Wenn Sie Screenshots von sozialen Medien machen und die Daten dokumentieren, beachten Sie, dass diese Daten zu echten Personen gehören. Wenn Ihre Systeme nicht sicher sind und die Daten in die falschen Hände geraten, können diese Personen ungewollt Gefahren ausgesetzt werden.
- Wenn Sie während Ihrer Verifizierung etwas auf geschlossenen oder anonymen Plattformen posten, verwenden Sie Ihren richtigen Namen?
- Werden Sie Ihre Absichten, warum Sie auf diesen Plattformen sind, ehrlich kundtun?

Weitere Informationen zu ethischen Fragen und verantwortungsvoller Berichterstattung finden Sie in First Drafts Leitfaden zum Thema Verantwortungsvolle Berichterstattung in Zeiten des Informationschaos¹ sowie im Kapitel Ethische Überlegungen in First Drafts Leitfaden zum Thema Geschlossene Gruppen, Nachrichten-Apps und Online-Werbung⁵.

KAPITEL 2

Herkunft

Was ist der Originalinhalt? Das ist die wichtigste Überprüfung im Verifizierungsprozess, die Sie immer zuerst durchführen sollten. Sobald man die Herkunft versteht, erschließen sich Kontext und Motivation. Wenn Sie den Inhalt nicht in der Form betrachten, wie er ursprünglich online erschien, könnten Sie übersehen, dass derselbe Inhalt einige Jahre früher das erste Mal in einem Artikel auftauchte. Vielleicht war er Bestandteil eines Running Gags auf 4chan oder entstand im Zuge einer koordinierten Kampagne in einer Facebook-Gruppe. Wenn Sie nicht das Original vor sich haben, dann könnten viele andere Details – wer es wann, wo, warum gepostet hat – auch falsch sein und den Rest Ihrer Verifizierung gefährden.

VORSICHT!

Es ist ganz einfach, Inhalt von einer Website oder Twitter herunterzuladen und diesen Inhalt dann auf eine andere soziale Plattform hochzuladen. Das nennt man Scraping und dadurch wird es schwieriger herauszufinden, ob Sie den Originalinhalt vor sich haben.

UMGEKEHRTE BILDERSUCHEN

Die umgekehrte Bildersuche ist ein Prozess, bei dem man leistungsstarke Software verwendet, um gleiche oder ähnliche Bilder in einer großen Datenbank wie Google Bilder zu finden. Wir verwenden die umgekehrte Bildersuche bei der Verifizierung sehr oft, das hat zwei Gründe.

- Visuelle Medien sind überzeugend, und deswegen erscheinen viele der effektivsten Fehlinformationen in Form von Fotos und Videos.

- Mit der umgekehrten Bildersuche finden wir die Herkunft heraus: den Ursprung der Inhalte oder zumindest ältere Versionen der Inhalte. Wenn Sie wissen, dass es ältere Versionen eines Bildes gibt, das im Netz als neu präsentiert wird, ist das ein direkter Hinweis darauf, dass es vielleicht aus dem Zusammenhang gerissen oder für einen anderen Zweck verwendet wurde oder ein Täuschung ist.

EIN LEITFADEN ZU DEN TOOLS

Die wichtigsten Suchmaschinen für die umgekehrte Bildersuche sind alle etwas unterschiedlich. Hier ist eine kurze Beschreibung der Unterschiede.

GOOGLE BILDER:

Der nützlichste Teil der Ergebnisse der umgekehrten Bildersuche von Google⁵ befindet sich ganz unten unter „Seiten, die die gleichen Bilder enthalten.“ Hier können Sie Artikel sehen, die das Foto zuvor verwendet haben. Es ist frustrierend, dass wir unsere Suchergebnisse mit Google nicht nach Datum ordnen können. Aber wir können einen spezifischen Datumsbereich auswählen, um die Ergebnisse einzugrenzen. Gehen Sie zu images.google.com, drücken Sie auf das Kamerasymbol im Suchfeld und laden Sie ein Bild hoch oder, wenn Sie Chrome verwenden, klicken Sie einfach mit der rechten Maustaste auf ein Bild und wählen Sie „bei Google nach Bild suchen“ aus.

YANDEX:

Die russische Suchmaschine Yandex⁶ hat eine große Datenbank und einige zusätzliche Funktionen, die Google nicht hat, wie Gesichter oder Bilder, die gespiegelt wurden, finden. Wenn Sie nichts bei Google finden, versuchen Sie es mit Yandex.

TINEYE:

Der Vorteil von TinEye⁷ besteht darin, dass Sie Ihre Suchergebnisse auf dieser Plattform leicht nach dem Datum ordnen können. Dadurch können Sie die erste dokumentierte Verwendung eines Fotos im Netz schnell sehen und dessen Herkunft besser verstehen. Nachteilig ist, dass die Suchmaschine eine wesentlich kleinere Datenbank mit Online-Fotos hat. Wenn Sie also nach etwas Unbekanntem suchen, gibt es das vielleicht nicht.

Unser --- meistempfohlenes Tool:

**DIE REVEYE REVERSE
IMAGE SEARCH EXTENSION
(CHROME⁸ ODER FIREFOX⁹).**

Mit der RevEye Browser Extension können Sie mit der rechten Maustaste auf ein Foto klicken und sofort eine Suche auf einer oder mehreren der oben gelisteten Plattformen durchführen oder auf allen gleichzeitig.

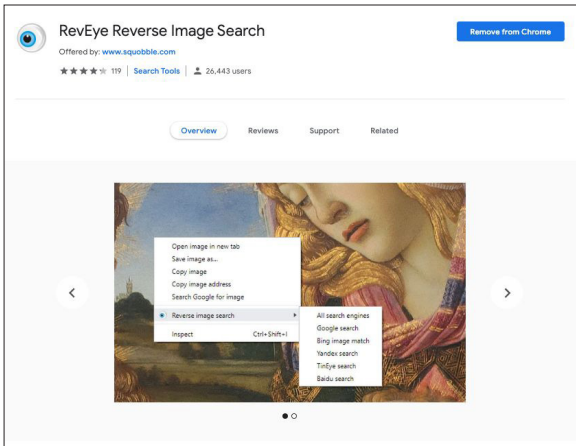


Abb. 2: RevEye Reverse Image Search ist im Chrome Web Store erhältlich. Abgerufen am 7. Sept 2019⁸. Screenshot der Autorin.

VIDEOVERIFIZIERUNG UND VERWENDUNG VON INVID

Die Suche nach der Herkunft von Videos verläuft ähnlich wie die Fotoverifizierung. Meist wird das erste Videobild als Thumbnail-Bild eines Videos verwendet – als Vorschaubild, bevor das Video startet – deshalb ist es nützlich, die Suche hier zu beginnen. Machen Sie einen Screenshot von einem Videobild und führen Sie damit eine umgekehrte Bildersuche wie bei jedem beliebigen anderen Bild durch.

Eines der besten Tools für die Verifizierung von Videos ist der InVID Verification Plug-in¹⁰, den Sie über eine Chrome oder Firefox Browser Extension verwenden. Hier sind einige seiner Merkmale:

- Die Herkunft eines Videos aus sozialen Medien lässt sich einfacher untersuchen, weil es in Thumbnails aufgeteilt wird, mit denen Sie mit einem Klick eine umgekehrte Bildersuche durchführen können.
- Sie erhalten allgemeine, mit dem Video verknüpfte Daten: das Hochlade-Datum und die Uhrzeit, Informationen zum Benutzerkonto, wie oft es geteilt und gelikt wurde sowie damit verbundenen Text.
- Durch natürliche Sprachverarbeitung werden Kommentare auf dem Video herausgefiltert, die für die Verifizierung nützlich sein könnten – mit anderen Worten Anmerkungen, die Hinweise geben könnten, ob es sich um ein Original, ein irreführendes oder ein aus dem Zusammenhang gerissenes Video handelt.
- Es gibt ein Lupen-Tool, mit dem Sie schnell kleingedruckten Text in einem Foto oder Video inspizieren können, wie das Kennzeichen am Rumpf eines Flugzeugs.

IN ANONYMEN FOREN NACH FRÜHEREN VERSIONEN SUCHE

Fehlinformationen, Memes und andere Arten von benutzergeneriertem Inhalt in sozialen Netzen stammen häufig aus geschlossenen und anonymen Foren. Wenn Sie nach der ersten Version eines Memes oder einer verdächtigen Behauptung suchen, lohnt es sich manchmal, in diesen Foren zu suchen.

- Prüfen Sie Reddit: Sie können die systemeigene Suchleiste verwenden oder ein Monitoring-Tool von Reddit wie [TrackReddit.com](https://www.trackreddit.com)¹¹.
- 4chansearch.com¹² ermöglicht Ihnen, 4chan und 4chan-Archivseiten zu durchsuchen.
- [Gab.ai](https://gab.ai)¹³ ist eine Art Alt-Twitter-Plattform mit vielen Benutzern, die gesperrt wurden.
- Discord-Kanäle, Facebook-Gruppen und WhatsApp-Gruppen lassen sich schwerer finden und durchsuchen, können bei tiefgehenden Untersuchungen aber die Mühe wert sein.

KAPITEL 3

Quelle

Wer hat den Originalinhalt aufgenommen? Wenn wir über die Verifizierung einer Quelle sprechen, unterscheiden wir, wer den Inhalt gepostet und wer ihn aufgenommen hat. Die Primärquelle ist die Person, die ihn aufgenommen hat. Es ist zum Beispiel durchaus möglich, dass jemand in Kairo ein Augenzeugenvideo auf seinem Telefon aufgenommen, es an einen Freund in Paris gesendet und dieser Freund es auf Twitter gepostet hat. Aber die Primärquelle ist der Augenzeuge in Kairo. Das ist derjenige, den wir idealerweise identifizieren möchten. Die Identifizierung von Primärquellen kann schwierig, aber für eine bessere Verifizierung durchaus lohnenswert sein. In diesem Kapitel erhalten Sie Tipps und Hinweise, wie das gemacht wird.

ALLGEMEINE FRAGEN ZU QUELLEN

- Wer ist der Hochladende?
- Sehen Sie sich andere Inhalte an, die er hochgeladen hat: Was erfahren Sie dadurch über den Account?
- Ist es möglich, dass er diesen Inhalt hochgeladen, aber nicht erzeugt hat?
- Ist es einleuchtend, dass die Person, der das Konto gehört, in der Nähe des Ortes war, als das Ereignis stattfand?
- Können Sie Kontaktinformationen finden? Suchen Sie nach einer Telefonnummer oder einer E-Mail-Adresse, damit Sie sich direkt an sie wenden können. Sie sollten mit der Quelle sprechen, bevor Sie Aussagen zu ihrer Identität treffen.

TIPPS ZUR UNTERSUCHUNG VON QUELLEN

Viele Menschen hinterlassen einen umfangreichen digitalen Fußabdruck, und es ist unglaublich, was Sie lernen können, wenn Sie die Zusammenhänge zwischen ihren verschiedenen Social-Media-Konten herstellen.

Hier sind einige Tipps:

- Sehen Sie sich den Benutzernamen des Kontos an und versuchen Sie, andere Kontennamen zu finden, die gleich sind.
- Führen Sie eine umgekehrte Bildersuche mit den Bildern im Konto durch.
- Suchen Sie nach Ausdrücken, die im Inhalt verwendet werden, um herauszufinden, ob es andere Konten gibt, die genau das gleiche Material posten.
- Wenn Sie Kontaktinformationen finden, die mit dem Konto verknüpft sind, geben Sie sie in eine Suchleiste ein, um herauszufinden, ob sie zu anderen Social-Media-Konten führen.
- Sie können bei Skype eine E-Mail-Adresse eingeben und es werden alle Benutzer angezeigt, die mit dieser E-Mail-Adresse verknüpft sind.
- Suchen Sie auf LinkedIn nach der Quelle, um hilfreiche, identifizierende Informationen zu finden.
- Viele Posts auf sozialen Netzwerken haben einen eindeutigen Identifikator, der sich normalerweise am Ende ihrer URL befindet. Sie können diesen Identifikator kopieren und bei Google einfügen, um herauszufinden, wo der Inhalt noch eingebettet wurde.
- Suchen Sie nach einer Website, die mit dem Social-Media-Konto verknüpft ist, und suchen Sie dort nach identifizierenden Informationen.

HANDELT ES SICH UM EIN AUTOMATISIERTES KONTO?

Es gibt zahlreiche Diskussionen zu Bots und viele Tools, die versuchen herauszufinden, ob Social-Media-Konten automatisiert sind oder nicht (zum Beispiel Hoaxy¹⁴ oder BotSentinel¹⁵). Aber Vorsicht: Die forensische Untersuchung von Bots ist keine exakte Wissenschaft.

Das müssen Sie wissen:

- Viele Tools benutzen 50 Tweets pro Tag als Maß, um zu bestimmen, ob es sich um ein automatisiertes Konto handelt. Natürlich gibt es viele nicht automatisierte Konten, die diese Anzahl mühelos übertreffen.
- Es ist weniger wichtig herauszufinden, ob ein Konto automatisiert ist oder nicht, sondern ob es kontinuierlich Fehlinformationen im Netz verbreitet – menschliche oder nicht menschliche.
- „Cyborgs“ sind Menschen, die sich bot-ähnlich verhalten, indem sie zum Beispiel den ganzen Tag lang häufig und regelmäßig posten. Einige Cyborgs werden für diese Arbeit bezahlt. Andere sind eifrige Anhänger einer bestimmten politischen Meinung oder eines politischen Kandidaten und sehen die Online-Amplifizierung als eine Aufgabe, die sie zur Unterstützung ihrer Sache übernehmen können.
- Wenn Sie daran interessiert sind, genauer herauszufinden, ob ein Konto automatisiert ist, liefert die Tweet-Aktivität im Laufe des Tages vielleicht ein besseres Maß. Die meisten Menschen müssen schlafen, was sich in einer Ruhephase ihrer Aktivitäten widerspiegelt. Auch das ist kein perfektes Maß, weil automatisierte Tweets so eingestellt werden können, dass sie nur während der Zeit erscheinen, in der Menschen normalerweise wach sind.

VERWENDUNG VON TWITONOMY, UM TWITTER-KONTEN ZU VERSTEHEN

Twitonomy¹⁶ ist ein ausgezeichnetes Tool, das wir für die Untersuchung von Twitter-Konten verwenden. Hier sind einige interessante Fragen zu Konten, die Sie mithilfe von Twitonomy beantworten können:

- Seit wann ist die Person bei Twitter und wie sieht ihr Tweet-Verlauf über einen längeren Zeitraum aus?
- Was ist ihre durchschnittliche Anzahl von Tweets pro Tag?
- Welcher Anteil ihrer Tweets wird retweetet?
- Welche Benutzer retweetet sie am häufigsten?
- Welchen Benutzern antwortet sie am häufigsten?
- Welche Hashtags verwendet sie am häufigsten?

DOMAINS UNTERSUCHEN

Manchmal möchten Sie herausfinden, wem eine bestimmte Website gehört. Es gibt viele Websites, die Ihnen dabei helfen, aber viewDNS.info¹⁷ ist unsere bevorzugte Website. Damit können Sie einfache Suchen nach Domains und IP-Adressen durchführen, aber auch andere Suchen, zum Beispiel nach historischen IP-Adressen für eine Domain sowie IP-Standortbestimmung.

Hier sind einige schnelle Tipps, wenn Sie Domains untersuchen:

- Wenn Sie die Authentizität einer Website infrage stellen, achten Sie auf verdächtige URL-Endungen.
- Hat der registrierte Nutzer dafür bezahlt, die Registrierdaten einer Domain zu verstecken, so müssen Sie nach alten Versionen der Website suchen. Manchmal findet eine Website-Migration statt und der registrierte Nutzer bezahlt für den Schutz der neuen Website, vergisst aber, die alte zu schützen. Sie können nach URL-Variationen suchen wie .net oder .info oder Sie können die Domain bei Google eingeben, um zu sehen, ob etwas Ähnliches angezeigt wird. Beachten Sie, dass diese Informationen in Europa automatisch durch die DSGVO geschützt werden.
- Sie können umgekehrte IP-Suchen durchführen, um sich andere Websites anzusehen, die auf demselben Server gehostet werden. Diese Websites stehen nicht unbedingt in einem Zusammenhang, aber die Ergebnisse können aufschlussreich sein.

TOOLS, IN DIE SIE INVESTIEREN SOLLTEN

Viele Tools, die wir früher zur Untersuchung von Social-Media-Benutzernamen verwendet haben, existieren nicht mehr, weil es berechtigte Bedenken hinsichtlich des Datenschutzes gab. Es gibt aber immer noch ausgezeichnete kostenpflichtige Tools, in die Sie vielleicht investieren sollten, wie Spokeo¹⁸ und Pipl¹⁹. Diese Verzeichnisse sind besonders hilfreich, um Kontaktinformationen zu finden.

KAPITEL 4

Datum

Wann wurde der Inhalt aufgenommen? Jeder Social-Media-Post hat einen Zeitstempel, aber Zeitstempel verraten Ihnen nur, wann ein Inhalt hochgeladen, nicht, wann er aufgenommen wurde. Durch eine strengere Verifizierung wird festgestellt, wann ein Inhalt aufgenommen wurde. Da Smartphones allgegenwärtig sind, passiert es oft, dass Personen Inhalte sofort nach dem Aufnehmen hochladen, aber Sie können nicht davon ausgehen, dass das immer der Fall ist. Es kann auch vorkommen, dass Nutzer die Inhalte anderer Personen ein paar Tage oder Jahre nach der Erstveröffentlichung erneut posten. Dieses Kapitel gibt Ihnen einige Tipps, wie Sie den Zeitpunkt der Aufnahme besser bestimmen können.

EIN LEITFADEN FÜR ZEITSTEMPEL IN SOZIALEN MEDIEN

Alle Plattformen zeigen Datum und Uhrzeit unterschiedlich an. Unten finden Sie praktische Erläuterungen dazu.



Reddit und 4chan zeigen die Uhrzeit und das Datum in der auf Ihrem Computer oder Gerät ausgewählten Zeitzone an, nicht die Lokalzeit des Nutzers, der die Nachricht gepostet hat.



Facebook und Twitter zeigen ebenfalls die Uhrzeit und das Datum in der auf Ihrem Computer oder Gerät ausgewählten Zeitzone an, nicht die Lokalzeit des Nutzers, der die Nachricht gepostet hat. Wenn Sie nicht eingeloggt sind, sehen Sie die Uhrzeit und das Datum in Pacific Standard Time (PST).

EXIF-DATEN

Eine weitere nützliche Methode, um die Zeit oder das Datum einer Aufnahme herauszufinden, ist die Betrachtung der Metadaten in der Datei.

Jedes mit einer digitalen Kamera aufgenommene Bild enthält zusätzliche Informationen in der Bilddatei, wie Uhrzeit, Datum, Kameraeinstellungen, Geräteinformationen und sogar Koordinaten, wenn das GPS des Gerätes eingeschaltet ist. Diese Daten bezeichnet man als Exif-Daten (Exchangeable image file format).

Ein phantastisches kostenloses Tool zur Anzeige der Exif-Daten einer Datei ist **Jeffrey's Exif viewer**²⁰. Laden Sie einfach eine Bilddatei hoch und die gespeicherten Extraintformationen werden angezeigt. Aber Vorsicht: Fast alle Social-Media-Plattformen entfernen die Exif-Daten, wenn ein Benutzer ein Bild hochlädt. Sie benötigen deswegen eine Originaldatei, damit es funktioniert. Wenn Sie Augenzeugeninhalte verifizieren, bitten Sie den Hochladenden, Ihnen die originale Bilddatei zu senden, damit Sie diese Überprüfung durchführen können.

▶ YouTube zeigt Uhrzeit und Datum in PST. Mit dem InVID Verification Plug-in können Sie die exakte Upload-Zeit in UTC sehen.

📷 Instagram zeigt nur ungefähre Uhrzeit und Datum des Uploads an, wenn Sie aber auf die drei Punkte (. . .) oben rechts klicken, zeigt der eingebettete Code die Zeit sowohl in PST als auch UTC an.

Das lohnt sich, wenn Sie den Bildern oder Dateien, die jemand gepostet hat, nicht trauen – und es funktioniert für unzählige Dateitypen. Natürlich lassen sich die Metadaten einer Datei fälschen oder ändern, aber nur Betrüger werden das versuchen.

TIPPS UND TOOLS VON PROFIS FÜR DIE VERIFIZIERUNG DES DATUMS

- Mit dem InVID Verification Plug-in²¹ können Sie die Upload-Zeiten von Videos auf soziale Medien in Coordinated Universal Time (UTC) sehen.
- SunCalc²² ermöglicht Ihnen, den Sonnenstand an einem bestimmten Tag an einem bestimmten Ort anzuzeigen. Damit lässt sich bestimmen, zu welcher Tageszeit etwas in einem Foto oder Video passiert ist.
- Wolfram Alpha²³ ist eine rechnergestützte Wissensmaschine, mit der Sie u. a. das Wetter an einem bestimmten Tag überprüfen können. Geben Sie einen Satz ein, zum Beispiel „Wie war das Wetter in Omaha am 5. November 2017“, um ein Ergebnis zu bekommen.
- Schauen Sie sich immer zuerst die Herkunft an. Führen Sie eine umgekehrte Bildersuche durch, wenn Sie visuelle Medien betrachten, um herauszufinden, ob es ältere Versionen des Inhalts gibt.

KAPITEL 5

Ort

Wo wurde der Inhalt aufgenommen? Social-Media-Posts werden häufig mit einem Geotag versehen, also einem Ort zugeordnet. Dabei handelt es sich nicht unbedingt um denselben Ort, an dem der Inhalt aufgenommen wurde. Geotags können falsch sein, Inhalt kann gespeichert und anderswo hochgeladen werden. Social-Media-Nutzer in tausenden Kilometern Entfernung können die Inhalte anderer Personen verwenden und posten, als wären es ihre eigenen. Dieses Kapitel hilft Ihnen zu verifizieren, wo der Originalinhalt aufgenommen wurde.

ALLGEMEINE FRAGEN ZUM ORT

- Wo ist das mit dem Inhalt verknüpfte Konto beheimatet?
- Wurde der Ort im Inhalt getaggt?
- Wenn der Ort identifiziert wurde, ist es einleuchtend, dass der Kontoinhaber dort war?
- Hat er seinen Ort in einem anderen Post angegeben?

STANDORTSUCHE AUF DEN PLATTFORMEN

Früher war es sehr einfach, innerhalb von Plattformen nach Orten zu suchen, aber aufgrund von Datenschutzbedenken wurden viele dieser Funktionen entfernt. Es gibt einige Tools von Drittanbietern, mit denen Sie solche Suchen immer noch durchführen können. Zum Beispiel das [whopostedwhat](#)²⁴-Instagram-Suchtool für Posts, die mit einem bestimmten Datum an einem bestimmten Ort getaggt sind. Viele dieser Drittanbietertools tauchen auf und verschwinden wieder. Deswegen ist es am besten, eine eigene Toolbox zusammenzustellen, die mit den Veränderungen und Aktualisierungen Schritt hält.

LASSEN SIE SICH NICHT TÄUSCHEN!

GEOTAGS KÖNNEN SIE AUSTRICKSEN

Manchmal sehen Sie, dass ein geografischer Ort mit einem bestimmten Tweet oder Facebook-Post verknüpft ist, aber diese Informationen lassen sich leicht manipulieren. Metadaten können ebenfalls manipuliert werden.

VERIFIZIEREN SIE ORTE IMMER UNABHÄNGIG

Wenn Sie sich ein Bild oder ein Video ansehen, suchen Sie den Ort auf einer Karte oder einem Satellitenbild, um Querverweise zu finden.

SELBST SATELLITENBILDER KÖNNEN FEHLERHAFT SEIN

Die Ortsbestimmung ist immer dann schwierig, wenn die relevanten Satellitenbilder veraltet sind. Aktuelle Ereignisse wie extremes Wetter oder Krieg können eine Landschaft in wenigen Minuten dramatisch verändern. Das erschwert die Ortsbestimmung von Videos in Ländern wie Syrien oder nach Wirbelstürmen.

BEOBACHTUNGSGABE SCHÄRFEN

Die wichtigste Fähigkeit für die Verifizierung eines Ortes ist die Beobachtungsgabe. Es ist erstaunlich, was Sie bezüglich der Ortsbestimmung herausfinden können, wenn Sie auf Details in Fotos und Videos achten.

Hier einige Fragen zum Warmwerden:

- Gibt es besondere geografische Merkmale? Große Straßen? Große Grünflächen? Berge?
- Gibt es besondere Gebäude, die auf Satellitenbildern leicht zu erkennen wären?

- Suchen Sie nach Telefonnummern, Nummernschildern, Geschäftsnamen und der Schrift auf Fahnen und Schildern.
- Untersuchen Sie den Kontext: Gibt es Veranstaltungen oder Situationen im Inhalt, die in Nachrichtenartikeln erscheinen könnten?
- Achten Sie auf Wetter, Vegetation und Kleidung – passen sie zu diesem Ort?

VERGLEICH MIT SATELLITENANSICHT UND STRASSENANSICHT

Hier sind einige Tools, die Sie kennen sollten, wenn Sie den Ort unabhängig verifizieren:

- Sie können nach Namen von Geschäften suchen und sich Orte in Satellitenansicht bei Google Maps²⁵ ansehen.
- Google Earth²⁶ ermöglicht Ihnen sogar, historische Satellitendaten zu betrachten.
- Wenn Sie sich intensiver mit Satellitenbildern beschäftigen möchten, können verschiedene Suchmaschinen nützlich sein, die Daten von verschiedenen Zeiten zur Verfügung stellen. Bing²⁷ und Yandex²⁸ sind zwei weitere Optionen. Yandex liefert mehr Daten aus Osteuropa.
- Wikimapia²⁹ ist ein interessantes Tool, das es der Community erlaubt, Merkmale auf der Karte zu beschreiben.

Häufig müssen bei der Ortsbestimmung mehrere verschiedene Merkmale in einem Bild oder einem Video identifiziert werden, die eingrenzen können, wo es aufgenommen wurde.

Die Vorwahl einer Telefonnummer auf einem Billboard ist ein guter Anfang. Zusammen mit einem Funkmast auf einem Hügel im Hintergrund und einem Dach im Vordergrund mit besonderer Form und Farbe haben wir eine viel bessere Chance, den Ort zu finden.

KAPITEL 6

Motivation

Warum wurde der Inhalt aufgenommen oder gepostet? Dieses Kapitel ist sehr kurz, weil es fast unmöglich ist zu verifizieren, warum jemand einen Inhalt aufgenommen und geteilt hat. Am besten wäre es, direkt zu fragen, und manchmal erfährt man selbst dann nicht die Wahrheit. Wenn man die Beweggründe versteht oder zumindest eine gewisse Ahnung hat, kann das sehr hilfreich für den restlichen Verifizierungsprozess sein.

Hier sind einige grundlegende Fragen zur Motivation:

- Bei Fotos und Videos: War die Person, die den Inhalt aufgenommen hat, zufällig Augenzeuge?
- Lässt sich aus dem Profil oder der Nutzung der sozialen Medien ableiten, dass es sich um einen Aktivist oder Unruhestifter handelt?
- Hat die Person eine Veranstaltung besucht, um sie unter einem bestimmten Blickwinkel aufzunehmen?
- Hat die Person Verbindungen zu einer Regierung, einem Unternehmen oder einer Forschungsorganisation?
- Ist die Person Mitglied in Online-Communitys, die eine bestimmte Sache unterstützen oder dafür werben?

STRENGE STANDARDS MÜSSEN EINGEHALTEN WERDEN

Denken Sie daran, dass Zitate oder Erklärungen, die im Netz veröffentlicht wurden, nicht so glaubwürdig sind wie ein direktes Interview mit der Quelle. Wenn es möglich und sicher ist, wenden Sie sich direkt an die Person, die den Inhalt aufgenommen hat.

DIE LIEBLINGSTOOLS VON FIRST DRAFT

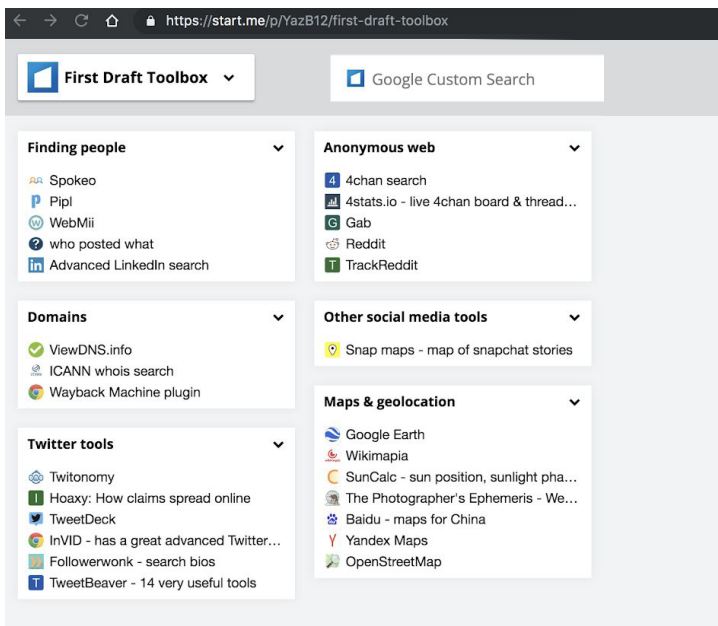





Abb. 4: First Draft Toolkit zeigt unsere am häufigsten eingesetzten Verifizierungstools. Abgerufen unter: bit.ly/FirstDraftToolkit. Abgerufen am 9. Dez. 2019. Screenshot der Autorin.






Shared







Photo verification ▼

-  RevEye Reverse Image Search plugin
-  Verexif - view & remove exif data
-  Karma Decay - rev img for Reddit
-  Yandex.Images: search for images o...
-  TinEye





Browser plugins ▼

-  InVID plugin
-  RevEye Reverse Image Search Plugin
-  Wayback Machine plugin
-  CrowdTangle Link Checker
-  Google Translate



Video verification ▼

-  InVID - swiss army knife of verifying ...
-  watch frame by frame
-  deturl - download youtube videos
-  YouTube Comment Scraper




Monitoring ▼

-  Spike - Monitor popular webpages o...
-  CrowdTangle -monitor FB, Tw, IG, & ...
-  Google Alerts
-  TrackReddit

Dates ▼

-  Time Zone Converter
-  Wolfram|Alpha - search for weather ...

Measuring spread ▼

-  BuzzSumo
-  Hoaxy: How claims spread online
-  CrowdTangle Link Checker

FUSSNOTEN

1. Kwan, V. (2019) *First Draft's Essential Guide to Responsible Reporting in an Age of Information Disorder*, London: First Draft. Abgerufen unter: https://firstdraftnews.org/wp-content/uploads/2019/10/Responsible_Reporting_Digital_AW-1.pdf
2. Wayback Machine plugin for Google Chrome. Abgerufen am 9. Oktober 2019. Unter: <https://chrome.google.com/webstore/detail/wayback-machinefpmgdkabkmnadcipehmlllkndpkmiak>
3. Hunchly. Abgerufen am 9. Oktober 2019. Unter: <https://www.hunch.ly/>
4. Dotto, C. & Smith, R. (2019) *First Draft's Essential Guide to Newsgathering and Monitoring on the Social Web*, London: First Draft. Abgerufen unter: https://firstdraftnews.org/wp-content/uploads/2019/10/Newsgathering_and_Monitoring_Digital_AW3.pdf
5. Dotto, C., Smith, R. & Wardle, C. (2019) *First Draft's Essential Guide to Closed Groups, Messaging Apps & Online Ads*. London: First Draft. Abgerufen unter: https://firstdraftnews.org/wp-content/uploads/2019/11/Messaging_Apps_Digital_AW-1.pdf
6. First Draft Toolbox auf Start.me. Abgerufen am 9. Oktober 2019. Unter: <https://start.me/p/YazB12/first-draft-toolbox>
7. Google Bildersuche. Abgerufen am 9. Oktober 2019. Unter: <https://www.google.com/imghp?hl=en>
8. Yandex Bildersuche Abgerufen am 9. Oktober 2019. Unter: <https://yandex.com/images/>
9. Tineye. Abgerufen am 9. Oktober 2019. Unter: <https://www.tineye.com/>
10. RevEye plugin for Google Chrome. Abgerufen am 9. Oktober 2019. Unter: <https://chrome.google.com/webstore/detail/reveye-reverse-image-sear/keaaclcjehbbapnphnmpikalfhelgf?hl=en>
11. RevEye plugin for Firefox. Abgerufen am 9. Oktober 2019. Unter: <https://addons.mozilla.org/en-GB/firefox/addon/reveye-ris/>
12. InVID Verification Plugin. Abgerufen am 9. Oktober 2019. Unter: <https://www.invid-project.eu/tools-and-services/invid-verification-plugin/>
13. TrackReddit. Abgerufen am 9. Oktober 2019. Unter: <https://www.trackreddit.com/>

14. 4chan Suche. Abgerufen am 9. Oktober 2019.
Unter: <http://4chansearch.com>
15. Gab. Abgerufen am 9. Oktober 2019. Unter: <http://Gab.ai>
16. Hoaxy. Abgerufen am 9. Oktober 2019.
Unter: <https://hoaxy.iuni.iu.edu/>
17. Bot Sentinel. Abgerufen am 9. Oktober 2019.
Unter: <https://botsentinel.com/>
18. Twitonomy. Abgerufen unter: <https://www.twitonomy.com/>
am 9. Oktober 2019.
19. ViewDNS. Abgerufen am 9. Oktober 2019. Unter: <https://viewdns.info/>
20. Spokeo. Abgerufen am 9. Oktober 2019.
Unter: <https://www.spokeo.com/>
21. Pipl. Abgerufen am 9. Oktober 2019. Unter: <https://pipl.com/>
22. Jeffrey's Exif Viewer. Abgerufen am 9. Oktober 2019.
Unter: <http://exif.regex.info/exif.cgi>
23. InVID Verficiation PlugIn. Abgerufen am 9. Oktober 2019. Unter:
[https://www.invid-project.eu/tools-and-services/
invid-verification-plugin/](https://www.invid-project.eu/tools-and-services/invid-verification-plugin/)
24. SunCalc. Abgerufen am 9. Oktober 2019.
Unter: <https://www.suncalc.org>
25. WolframAlpha. Abgerufen am 9. Oktober 2019.
Unter: <https://www.wolframalpha.com/>
26. WhoPostedWhat. Abgerufen am 9. Oktober 2019.
Unter: <https://whopostedwhat.com/>
27. Google Maps. Abgerufen am 9. Oktober 2019.
Unter: <https://www.google.com/maps>
28. Google Earth. Abgerufen am 9. Oktober 2019.
Unter: https://www.google.co.uk/intl/en_uk/earth/
29. Bing Maps. Abgerufen am 9. Oktober 2019.
Unter: <https://www.bing.com/maps>
30. Yandex Maps. Abgerufen am 9. Oktober 2019.
Unter: <https://yandex.com/maps/>
31. Wikimapia. Abgerufen am 9. Oktober 2019.
Unter: <https://wikimapia.org>

ÜBER FIRST DRAFT

First Draft ist eine globale, gemeinnützige, unparteiische Organisation zur Unterstützung derjenigen, die in der Berichterstattung an vorderster Front stehen. Wir stellen praktische Ratschläge und Schulungen bereit, die auf kontinuierliche Forschung gestützt sind. Fertigkeiten, Tools und Empfehlungen werden gemeinsam mit Partnern in aller Welt ständig getestet und überarbeitet.

FIRSTDRAFT

Unterstützt durch

Google News Initiative

@firstdraftnews

Weitere Informationen unter firstdraftnews.org/resources